Health and Human Services Agency
CalOHII
California Office of Health Information Integrity

SUMMARY OF COMMENTS
CALPSAB MOTIONS AND INTERIM
HIE PRIVACY AND SECURITY GUIDELINES
December 2009

The following summarizes the comments received during the public comment period which ended on December 1, 2009 on the Interim HIE Privacy and Security Guidelines. Approximately 33 organizations and 1, 232 individuals provided comments.

Adequacy of Patient Privacy Protections in the Guidelines

Two differing perspectives were threaded through the comments:

The guidelines and current law **do not provide adequate protections** for patient privacy because they require patients to take affirmative steps to "opt out" of the sharing of their medical records through health information exchanges without the potential of their understanding and full explicit, informed consent. Commenters stated:

- Need to have full opt-in informed consent during transition from paper to HIE to create and maintain patient trust.
- Receivers of individual health information, particularly sensitive information should maintain the confidentiality of the information after receipt.
- PRCH has recorded 340,242,628 personal records breached since 2005 of which health information may have been included. Electronic health exchange will increase the potential for more breaches.
- Need to address the use of de-identified health information through an HIE.

Current law **adequately addresses** patient privacy:

- Robust, comprehensive, and detailed safeguards already exist to safeguard patients health information; notices of privacy practices, minimum necessary standard, privacy and security policies and procedures, security rules, accounting of disclosures and breach notification.
- To the extent health information is being improperly accessed, measures should be taken to address the situation directly.

Sensitive Health Information

Commenters generally believed that sensitive health information should have additional protections, but were challenged on how to accomplish such protections with the intermingled records:

- Opt in for sensitive information is absolutely essential except in emergency situations.
- Intermingled records prevent segregation of sensitive information; therefore, requiring all health information be shared on an opt in basis would provide patient permission for the exchange.

- Consent for sensitive information must be consistent with the requirements of law.
- Should include information about which individuals have real world privacy concerns, not just that specifically protected by law.
- Need higher standards for reproductive health information and health information resulting from abuse.
- Need to inform providers of missing sensitive health information to:
  - Support trust of HIE data
  - Avert patient safety issues
  - Provide opportunity to obtain information from patient.

Hybrid Bi-Lateral Patient Consent Policy

CalPSAB Recommended Policy: No consent for mandated public health exchanges, opt out for clinical treatment and opt in for all other uses. The commenters generally believed the policy recommended by the CalPSAB cannot be operationalized. The policy*:*

- Is confusing to both patients and providers and unnecessarily administratively burdensome.
- Seems to undermine the HIPAA requirements for sending required health care transactions electronically and in a timely fashion; is not consistent with the consent option provided to covered entities in HIPAA
- Does a disservice to consumers and system by installing unneeded barriers to the exchange of health information when it is legal, appropriate, and beneficial to the patient.
- Would provide an inconsistent platform of HIE-consent for multi-state provider systems
- Increases costs for all involved
- May inhibit compliance with other laws; Knox-Keene Act for continuity of care, quality assurance and emergency services.
- Is impossible for physicians to operationalize - not technically feasible at this time for existing HIT systems

Opt In Support

Some commenter expressed support for the opt in patient consent policy and provided reasons why the opt out patient consent policy was not sufficient:

- Should allow the patient to opt in at the point of care in any venue without placing an undue burden on the provider.
- Personal health information belongs to an individual thus he/she have the right to decide when and how it is shared. Patients have the right to affirmatively opt in after being convinced that adequate safeguards are in place; trust must be earned.
- Patients may not fully understand that failure to opt out results in rapid and broad dissemination of their information through the HIE and the potential consequences of such dissemination.
- Patients may fail to opt out because they forget, are rushed
- Does not force patients to forgo, delay, or abandon treatment for mental illness, STDs, and anything that has a stigma attached to it if they have no confidence they can control that information; does not force patients to choose between privacy and health care
- Rapid and broad dissemination of individual health information will result in bigger mistakes/breaches.
- Is consistent with historical practices, patients do not expect their physician to obtain prior records without being specifically asked.
- Opt in is needed until the system details are worked out.
- Enhances patient trust of HIE
- Is essential for sensitive health information; opt out does not comport with the legal (Article 1, Section 1 of the California Constitution) and ethical requirements for the transmission of sensitive health information.
- Patients with disabilities should be adequately informed and have the ability to specifically consent to disclosure of information to provide other than their own provider due to concern of stigma and discrimination based on the individual's disability.
- An opt out approach may increase the risk and magnitude of lawsuits against providers and other entities that do not adequately control patient data while opt in mitigates this risk
- An opt out approach will likely lead to significant disclosures of sensitive health information without patient consent due to the intermingled records that currently exists in EHRs.
- Allows patients to seek prompt treatment for health conditions, including stigmatizing conditions.

- Reduces need to segregate health information due to levels of sensitivity

Opt Out Support

Other comments expressed support for an opt-out patient consent policy or, in some cases, a no consent policy:

- There will be a higher adoption rate; is less costly
- Critical to success rate for physician adoption; providers will not participate in HIE if opt in is required due to task of collecting and tracking patient consent choices
- Best facilitates timely adoption of HIT; opt in will impede further adoption of HIE/HIT
- *Consistent with existing legal framework;* Opt-in is not a HIPAA requirement, and the opt-in requirements have already been rejected by both the federal government (HIPAA regulation changes in August 2002) and leading consumer organizations (CDT; Rethinking the Role of Consent in Protecting Health Information Privacy: January, 2009).
- Does support consumer choice – may opt out
- Supports larger goal of improved health outcomes
- Information for legally allowed purposes should be shared through an HIE without patient consent, however, the network should have the capability to segregate and provide differential access to the information based on the patient's stated preferences or sensitivity to the information.
- Patients should have the ability to opt out of any data collection by an HIO that retains individually identifiable health information.
- Support of opt out conditioned on structural limits on allowed uses of HIE, and prerequisites for authorized access to an HIE existing; setting and enforcing limits on data collection, use, and disclosure, ensuring patient's access to information and rigorous user authentication.

Limitation of Uses and Disclosures

Some commenters believed that the limitations on uses and disclosures for the HIE were too limited while others saw the need to balance the limitation on uses and disclosures with security controls and consent policies:

- Limiting the use and disclosure of data to treatment is not realistic and will negatively impact patient care decisions.
- Exchanges for other activities such as case management, quality reporting, peer review activities, DMHC required reporting, performance reporting, pay for performance program, and payment and communications with payers are necessary

which are vital uses to entities ability to remain in the care arena and essential to providing high quality care

- Recommend that permitted uses for HIE be slightly expanded to include those necessary to establish meaningful use; recommend that the use limitations be expanded to include those allowed for the NHIN in the DURSA
- Concerns were expressed inability to exchange data for health care operations.
- Should include those exchanges required to allow an HIO to facilitate the exchange
- Uses and disclosures made outside of the HIE of individual health information should not be limited as provided in the Guidelines (Section 3.3).

Authority and Applicability of Guidelines

Commenters questioned the authority and scope of applicability of the guidelines:

- It is unclear to whom the guidelines apply and the scope of that application.
  - Unclear whether the guidelines will apply to the transmission of individual health information within a medical group or an Independent Physicians Association (IPA), between its doctors, administrators, and affiliates.
  - Unclear whether the guidelines apply to the exchange between a provider group and
  - Unclear whether the guidelines apply to a hospital, or between two provider groups in continuity of care records request.
- May, in a sense, create a law without going through the Legislative process.
- It is unclear what authority the guidelines will have with regard to enforcement.
- Question the legality of linking compliance with the Guidelines to receipt of HITECH funding.
- The Guidelines do not have the power of law; specific parts of the guidelines need amendments of existing state and/or federal law to be effective, e.g., consent, limitation of uses for HIE, break-the-glass, sensitive information limitations, .

Minimum Necessary

Several commenters expressed concerns around the minimum necessary requirements in the Interim Guidelines:

- Sensitive health information disclosures should provide the least amount of information possible to satisfy the need or request; on a need to know basis.
- Provisions should include the minimum necessary individual health information used and disclosed.

- Should not impose undue burdens on providers and health care delivery through a minimum necessary standard for health information used for treatment purposes or through complex and time consuming consent requirements.

Security

Comments were received concerning the security portion of the guidelines:

- Recommend adoption of strict security controls that ensure that organizations and participants in HIE networks are:
    - Properly authenticated
    - Provide access only to information appropriate to role and relationship to the subject of the information
    - Hold accountable for adhering to privacy and security standards.
- Dual factor authentication will shut out the non-affiliated physicians and safety net physicians.
- Need to clarify which entity is responsible for authentication; the requestor or the HIO.
- Need more robust internal access controls to limit the dissemination of patient information to only those actually involved in treatment.
- Need to define “data source” and “data subject” in relation to the Access Control policy.

Education

Several comments were received concerning the need for education for both the patients as well as those to whom the guidelines will apply:

- Should provide clear patient notice requirements for HIEs.
- Should facilitate the development of strong programs to educate the public regarding HIE.
- Provision of sample forms would lessen the complexity of the guidelines.
- Patients need to be notified of their ability to provide consent in a way that is comprehensive, but addresses language, education, and reading ability.

Barriers to Adoption of HIE

Several commenters provided information about barriers that may/do exist to implement, operationalize, and adopt the guidelines.

- Provider inability to operationalize the guidelines.
  - Current level of technology and administrative capability does not allow for varying standards of opt in/opt out based on the type of individual information and may not for several years.
  - May force providers to exclude patients that are unwilling to accept an opt-out arrangement, limiting their choice of providers and access to medical care.
- Bi-Level consent will cause providers to opt out of HIE rather than take on the extraordinary task of collecting and tracking the patients' consent choices..
- Go beyond what is reasonably necessary to maintain patient privacy
- Hurts patients by hindering physicians' adoption of HIE; already poses challenges given the costs, interoperability problems and other technological burdens.
- Will impede the adoption of HIT contrary to national and statewide efforts to promote quality and reduce costs.

Guideline Framework

Commenters also provided comments on the guidelines in general. These comments included: the guidelines were unnecessary; California should rely on the national standards only, or California should rely on HIPAA and State law as they exist. Others thought that the guidelines should address only the gaps that currently exist in current State law and HIPAA that govern the use and disclosure of individual health information through an HIE. Some were concerned with the ability to implement the guidelines and how they related to HIPAA and State law. One feared that the guidelines would lead to "when in doubt, don't share."